THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE
PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1.   A method for determining a result of a group operation performed an integral
number of times on a selected element of the group, said method comprising the steps of
:

    (a) representing said integral number as a binary vector;

    (b) initializing an intermediate element to the group identity element;

    (c) selecting successive bits, beginning with a left most bit, of said vector and
        for each of said selected bits;

        (i)   performing said group operation on said intermediate element to
            derive a new intermediate element;

        (ii) replacing said intermediate element with said new intermediate
            element;

        (iii) performing said group operation on said intermediate element
            and an element, selected from the group consisting of:

                said group element if said selected bit is a one; and

                an inverse element of said group element if said selected bit
                is a zero;

        (iv) replacing said intermediate element with said new intermediate
            element;

    (d) performing said group operation on said intermediate value and said
        inverse element if said last selected bit is a zero; and replacing said
        intermediate element therewith, to obtain said result, whereby each of the
        bits of said integral is processed with substantially equal operations
        thereby minimizing timing attacks on said cryptographic system.

2. A method as defined in claim 1, said group being a multiplicative group $F_p{}^*$ said
group element being an integer, and said group operation being exponentiation g^a and
an inverse element being the multiplicative inverse $1/g$.